UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/811,323	03/26/2004	Tao Li	1118.70214	9463

7590 10/23/2007

Patrick G. Burns, Esq.
GREER, BURNS & CRAIN, LTD.
Suite 2500
300 South Wacker Drive
Chicago, IL 60606

EXAMINER	
HOFFMAN, BRANDON S	

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
10/23/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

D

Office Action Summary	**Application No.** 10/811,323	**Applicant(s)** LI ET AL.
	Examiner Brandon S. Hoffman	**Art Unit** 2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 March 2004*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *26 March 2004* is/are: a)□ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.☒ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *8-12-04*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. Claims 1-4 are pending in this office action.

Priority

2. Receipt is acknowledged of papers submitted under 35 U.S.C. 119(a)-(d), which papers have been placed of record in the file.

Information Disclosure Statement

3. The information disclosure statement (IDS) submitted on August 12, 2004, is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Drawings

4. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(4) because reference characters "21" and "12" have both been used to designate interface. Specifically, figures 1 and 8 have interface 21, while figure 5 has interface 12. Examiner believes it to be a typo for interface 12 which would need to be replaced with interface 21. Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. Each

drawing sheet submitted after the filing date of an application must be labeled in the top margin as either “Replacement Sheet” or “New Sheet” pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Specification

5. Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

Specifically, the abstract is longer than 150 words and needs to be shortened.

Appropriate correction is required.

Claim Rejections - 35 USC § 101

6. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 3 and 4 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claims 3 and 4 recite a digital signature generation request program for a computer and a digital signature authentication request program for a computer, respectively. The limitations that follow simply list steps that the computer performs in response to the program. As is known, a program is software, and therefore is intangible.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1-4 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bowe et al. (U.S. Patent Pub. No. 2003/0093678) in view of Parmelee et al. (U.S. Patent Pub. No. 2002/0128969).

Regarding claim 1, Bowe et al. teaches a digital signature generation method for generating a digital signature for electronic information existing on a storage unit of a terminal in a system configured to enable said terminal and a server device to communicate with each other via a network, said method comprising steps of:

- Sending, from said terminal to said server device, the Digest value and identifying information of a user as an issuer of the electronic information (fig. 1 and paragraph 0056);
- Taking, in said server device, a secret key corresponding to the identifying information received from said terminal, out of a storage device stored with a pair of a secret key and a public key related with identifying information of each user (paragraph 0054 [using the clients key stored on the server] and 0057);
- Generating, in said server device, a signature value by encrypting the Digest value received from said terminal with the secret key taken out of said storage device (fig. 2 and paragraph 0059); and
- Responding, from said server device to said terminal, the generated signature value (fig. 2, SIGNING RESPONSE and paragraph 0058).

Bowe et al. does not teach calculating, in said terminal, a Digest value for the electronic information or forming, in said terminal, undersigned electronic information by attaching the signature value and the identifying information responded from said server device to the electronic information.

Parmelee et al. teaches calculating, in said terminal, a Digest value for the electronic information (fig. 10, ref. num 326/334) and forming, in said terminal, undersigned electronic information by attaching the signature value and the identifying information responded from said server device to the electronic information (paragraph 0066).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine calculating a digest value of the electronic information and attaching the signature value to the electronic information, as taught by Parmelee et al., with the method of Bowe et al. It would have been obvious for such modifications because calculating a digest saves before transmission of the data saves bandwidth by transmitting a smaller data that represents a larger data. Attaching the server created digital signature to the electronic document provides non-repudiation of the document.

Regarding claim 2, Bowe et al. teaches a digital signature authentication method for authentication undersigned electronic information obtained by said digital signature generation method according to claim 1, in a system configured to enable said terminal and a server device to communicate with each other via a network, said method comprising steps of:

- Sending, from said terminal to said server device, the Digest value, and a signature value and the identifying information in the undersigned electronic information (fig. 3, VERIFICATION REQUEST AND SIGNED OBJECT and paragraph 0060);

- Taking, in said server device, a public key corresponding to the identifying information received from said terminal, out of said storage device (paragraph 0016, use their public key);
- Decrypting, in said server device, the signature value received from said terminal with the public key taken out of said storage device (paragraph 0016, decrypt the hash);
- Comparing, in said server device, a substance of the decrypted signature value with the Digest value received from said terminal (paragraph 0060, determining if signatures match); and
- Responding, by said server device, a result of the comparison to said terminal (fig. 3, VERIFICATION RESPONSE AND INDICATOR and paragraph 0060).

Bowe et al. does not teach calculating, in said terminal, a Digest value for the electronic information.

Parmelee et al. teaches calculating, in said terminal, a Digest value for the electronic information (fig. 10, ref. num 326/334).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine generating a Digest value for the electronic information, as taught by Parmelee et al., with the method of Bowe et al. It would have been obvious for such modifications because calculating a digest saves before transmission of the data saves bandwidth by transmitting a smaller data that represents a larger data.

Regarding claim 3, Bowe et al. teaches a digital signature generation request program for a computer communicable via a network with a server device including a storage device stored with a pair of a secret key and a public key related with identifying information of each user, said computer taking, when receiving a digital signature generation request message designating encryption object information and identifying information, the secret key corresponding to the received identifying information out of said storage device, generating a signature value by encrypting the encryption object information with the secret key and responding the generated signature value, said program making said computer:

- If electronic information and identifying information of a user as an issuer of the electronic information are specified (fig. 1, paragraph 0056, fig. 2, ref. num 210 and paragraph 0058),
- Send the digital signature generation request message containing the calculated Digest value as the encryption object information and the identifying information to said server device (fig. 2);

Bowe et al. does not teach calculating, in said terminal, a Digest value for the electronic information or if the signature value is responded from said server device, form undersigned electronic information by attaching the signature value and the identifying information to the electronic information.

Parmelee et al. teaches calculating, in said terminal, a Digest value for the electronic information (fig. 10, ref. num 326/334) and if the signature value is responded from said server device, form undersigned electronic information by attaching the signature value and the identifying information to the electronic information (paragraph 0066).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine calculating a digest value of the electronic information and if the signature value is responded, attaching the signature value to the electronic information, as taught by Parmelee et al., with the program of Bowe et al. It would have been obvious for such modifications because calculating a digest saves before transmission of the data saves bandwidth by transmitting a smaller data that represents a larger data. Attaching the server created digital signature to the electronic document provides non-repudiation of the document.

Regarding claim 4, Bowe et al. teaches a digital signature authentication request program for a computer communicable via a network with a server device including a storage device for stored with a pair of a secret key and a public key related with identifying information of each user, said computer taking, when receiving a digital signature authentication request message designating authentication object information, signature value and identifying information, the public key corresponding to the received identifying information out of said storage device, decrypting the signature value with the public key, comparing the decrypted signature value with the authentication object information, and responding a result of the comparison, said program making said computer:

- If undersigned electronic information obtained according to claim 1 or 3 is inputted, send the digital signature authentication request message containing the Digest value as the authentication object information and the signature value and the identifying information in the undersigned electronic information to said server device (fig. 3 and paragraph 0060).

Bowe et al. does not teach calculating, in said terminal, a Digest value for the electronic information.

Parmelee et al. teaches calculating, in said terminal, a Digest value for the electronic information (fig. 10, ref. num 326/334).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine calculating a digest value for the electronic information, as taught by Parmelee et al., with the program of Bowe et al. It would have been obvious for such modifications because calculating a digest saves before transmission of the data saves bandwidth by transmitting a smaller data that represents a larger data.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon S. Hoffman whose telephone number is 571-272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Brandon Hoffman/

BH